

SK:DEL

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
DROPBOX USER IDENTIFICATION
NUMBERS 26293153, 1208420448 AND
1719104928 THAT IS STORED AT
PREMISES CONTROLLED BY DROPBOX
INC.

**APPLICATION FOR A
SEARCH WARRANT FOR
INFORMATION IN
POSSESSION OF DROPBOX INC.**

Case No. 20-MJ-308

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, CHRISTINE CULLEN, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Dropbox Inc. (“Dropbox”), specifically accounts for Dropbox User Identification Numbers 26293153, 1208420448 and 1719104928 (the “SUBJECT ACCOUNTS”).

2. Dropbox is a provider of electronic communications services, as defined in 18 U.S.C. § 2510(15), and/or remote computing services, as defined in 18 U.S.C. § 2711(2). Dropbox is headquartered in San Francisco, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Postal Inspector with the United States Postal Inspection Service (USPIS), and assigned to a Mail Fraud team in the New York division. I have been employed by the USPIS since June 2017. As a Postal Inspector, I am charged with investigating violations of the laws of the United States, collecting evidence in cases in which the United States is or may be a party in interest, and performing other duties imposed by law. More specifically, I investigate crimes involving the misuse of the mail system in furtherance of certain frauds, schemes and swindles. As part of my responsibilities as a Postal Inspector, I have attended various classes and training including a 12-week Basic Inspector Training, mail fraud training, and financial crimes training.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to search the information described in Attachment A for evidence, fruits or instrumentalities of violations of Title 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), 1349 (conspiracy to commit mail and wire fraud), 2320(a)(4) (conspiracy to commit trademark counterfeiting), and 1956 (laundering of monetary instruments) (the “SUBJECT OFFENSES”).

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a),

(b)(1)(A) and (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that . . . has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

MANUFACTURER COUPON COUNTERFEITING

7. Manufacturing companies, such as Procter and Gamble, issue legitimate manufacturer coupons to consumers with a save value embedded in the barcode. Manufacturer coupons contain certain terms and disclaimers indicating that they are not to be transferred, sold, reproduced or altered, and that doing so is illegal. However, there are many online communities dedicated to the unlawful creation, replication and/or alteration of coupons. There are various websites and blogs dedicated to instructing consumers how to effectively “glitch, glitter or balance” coupons, all terms referring to the illegal, and intentional, misuse of coupons. Many of these websites lead to forums and social media groups dedicated to the buying and trading of counterfeit coupons.

MANUFACTURER COUPON PROCESSING

8. When a customer makes a purchase utilizing a manufacturer coupon, the retailer accepts the coupon and applies the coupon discount for the customer at the time of payment. The retailer then sends the redeemed coupon to their clearinghouse, which is a processing center for all manufacturer coupons redeemed at the retailer. At the clearinghouse, the coupons are scanned to determine if they are legitimate or counterfeit. This is determined by an offer code, a unique six-digit identifier embedded in the barcode of every coupon. Offer codes are established by the manufacturer. If the offer code does not exist or is redeemed for a value other than the manufacturer’s intended value, the coupon is flagged as counterfeit. The clearinghouse tallies all the redeemed coupons, and generates an invoice to the manufacturer indicating how much is owed to the retailer for the redeemed

coupons. At that point, the manufacturer reimburses the retailer for the legitimate coupons and determines if the retailer should be reimbursed for any counterfeit coupons.

IDENTIFICATION OF THE TARGETS

9. There is probable cause to believe that JAMES PEARSON and CATHERINE PEARSON (together the “TARGETS”) are selling counterfeit coupons online. The TARGETS’ residence is located at 4 Oakmont Road, Beverly, MA 01915 (the “TARGETS’ RESIDENCE”). According to Comcast records obtained by subpoena, the TARGETS’ RESIDENCE has a registered Internet Protocol (“IP”) address of 73.143.79.13 (the “TARGETS’ IP ADDRESS”).

10. For instance, between January 2018 and August 2018, both dates being approximate and inclusive, an undercover buyer (herein the “UCB”) made eight (8) counterfeit manufacturer coupon purchases from the TARGETS, resulting in the acquisition of 449 counterfeit manufacturer coupons. The UCB spent \$581.00 for these coupons and received \$9,139.44 in manufacturer coupon value. In other words, for every \$1.00 spent for the purchase of counterfeit manufacturer coupons, the UCB received \$15.73 in manufacturer coupon value. Each UCB purchase is detailed in the Premises Search Warrant, Case No. 19-1274, signed by the Honorable Donald L. Cabell of the United States District Court for the District of Massachusetts, on November 4, 2019 (attached hereto as Exhibit A).

11. On November 4, 2019, Judge Cabell signed a search warrant authorizing law enforcement agents to search the TARGETS’ RESIDENCE, for evidence, fruits and instrumentalities of violations of Title 18 U.S.C. §§ 1341 (mail fraud), 1349 (conspiracy to commit wire fraud), 2320(a)(4) (conspiracy to commit trademark counterfeiting), and 1956 (laundering of monetary instruments).

12. Based on digital evidence collected from the TARGETS' RESIDENCE, Dropbox applications were installed and utilized on both computer and iPhone devices owned and operated by the TARGETS.

13. A review of hard drives collected from the TARGETS' RESIDENCE found numerous files containing manipulated coupon barcodes, templates and images; spreadsheets indicating details of coupon orders that customers had placed; and video tutorials showing how to manipulate coupons for fraudulent use. In addition, thousands of file paths such as "Windows/users/ethan/dropbox/coupon template/lowerbar/.75 softsoap 030218.png" and "Windows/users/cathy/dropbox/coupon template/foils/20180510 foil-always 699.pdf" were discovered, indicating the TARGETS have been storing coupon templates in the SUBJECT ACCOUNTS on Dropbox.

14. According to Dropbox records obtained by subpoena, the SUBJECT ACCOUNTS are associated with the following email addresses: blinkieguy@gmail.com, Cathynjames5@gmail.com, and Jamespearson101@gmail.com.

15. According to Google records obtained by subpoena, between July 2017 and December 2018, both dates being approximate and inclusive, the above e-mail addresses (blinkieguy@gmail.com, Cathynjames5@gmail.com, and Jamespearson101@gmail.com) were registered and/or accessed by a user at the TARGETS' IP ADDRESS. Accordingly, there is probable cause to believe those are the TARGETS' email addresses, and the TARGETS used them to register for the SUBJECT ACCOUNTS.

BACKGROUND CONCERNING DROPBOX

16. “Dropbox” refers to an online storage medium on the internet accessed from a computer or electronic storage device via the Internet. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved electronic files without having to store those files on their own computer or other electronic storage device. Dropbox is an “offsite” storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their electronic files on Dropbox and avoid having those files appear on their computer. Anyone searching an individual’s computer that utilizes Dropbox would not be able to view these files if the user opted only to store them in an online storage medium, such as Dropbox.

17. Dropbox provides a variety of online services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers (Dropbox offers both free and pay services), means and source of payment (including any credit or bank account number).

18. When the subscriber transfers a file to a Dropbox account, it is initiated at the user’s computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox

servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

19. Online storage providers like Dropbox typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

20. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

21. As explained herein, information stored in connection with a Dropbox account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion.

22. For these reasons, as further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the SUBJECT OFFENSES, but also forensic evidence that establishes how the SUBJECT ACCOUNTS were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be in the SUBJECT ACCOUNTS because:

- a. Data in a Dropbox account can provide evidence of a file that was once in the account but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information in the account that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information in the account that can reveal information such as online nicknames and passwords.
- b. Forensic evidence in an account can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how a Dropbox account works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the SUBJECT ACCOUNTS was used, the purpose of its use, who used it, and when.
- d. The process of identifying the exact electronically stored information in a Dropbox account that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored in a Dropbox account is evidence may depend on other information stored in the account and the application of knowledge about how a Dropbox account works. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a Dropbox account was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present in an account.
- f. I know that when an individual uses a Dropbox account, the individual’s account can generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The account is

an instrumentality of the crime because it is used as a means of committing the criminal offense. The account is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a Dropbox used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

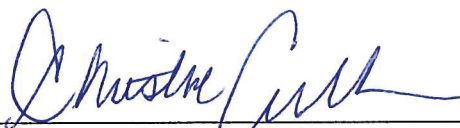
CONCLUSION

22. Based on the forgoing, there is probable cause to believe that within the SUBJECT ACCOUNTS, evidence of violations of the SUBJECT OFFENSES exists.

Accordingly, the government requests a search warrant for the SUBJECT ACCOUNTS.

23. Because the warrant will be served on Dropbox, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



CHRISTINE A. CULLEN
US Postal Inspector
United States Postal Inspection Service

Subscribed and sworn to before me on April 10, 2020



THE HONORABLE CHERYL POLLAK
CHIEF UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with accounts for Dropbox User Identification Numbers 26293153, 1208420448 and 1719104928 (the “SUBJECT ACCOUNTS”) that are stored at premises controlled by Dropbox, a company that is headquartered at 333 Brannan Street, San Francisco, California 94107.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by Dropbox (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;
- b. The contents of any hyperlinks sent to or from the account;
- c. All transactional information of all activity of the Dropbox accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting; and emails “invites” sent or received via Dropbox, and any contact lists.
- d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of

service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

- e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. All records pertaining to communications between Dropbox and any person regarding the account or identifier, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 21 days of service of this warrant.

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), 1349 (conspiracy to commit mail and wire fraud), 2320(a)(4) (conspiracy to commit trademark counterfeiting), and 1956 (laundering of monetary instruments) (the “SUBJECT OFFENSES”), involving the user(s) of the SUBJECT ACCOUNTS, their co-conspirators and associates, and occurring after January 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Evidence of the creation, possession, receipt, transportation, reproduction and distribution of counterfeit coupons in violation of 18

U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud) 1349 (conspiracy to commit mail and wire fraud), 2320(a)(4) (conspiracy to commit trademark counterfeiting), and 1956 (laundering of monetary instruments) (the “SUBJECT OFFENSES”), including coupon barcodes, templates and images; documents containing customer details, including spreadsheets indicating coupon orders; and video tutorials on coupon manipulation;

- b. Evidence indicating how and when the SUBJECT ACCOUNTS were accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the SUBJECT ACCOUNTS’s owner(s);
- c. Evidence of who used, owned, or controlled the SUBJECT ACCOUNTS at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence. User attribution information (i.e. files and other data such as chats or e-mails) will tend to show the identity of the person using the SUBJECT ACCOUNTS near the time of the criminal activity;
- d. Evidence relating to SUBJECT ACCOUNTS use of any IP addresses;
- e. Evidence indicating the SUBJECT ACCOUNTS’s owner’s state of mind as it relates to the crimes under investigation;

- f. The identity of the person(s) who communicated with the user ID possession, in relation to the creation, purchase, or sale of coupons, including records that help reveal their whereabouts.

Exhibit A

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for the Premises at 4 Oakmont Drive., Beverly, MA, and Any Closed Containers/Items Contained Therein, and Electronic Devices.

TO BE FILED UNDER SEAL

Case No. 19-mj-1274-DLC

AFFIDAVIT IN SUPPORT OF SEARCH AND SEIZURE WARRANT

Kate E. Hanecak, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I am a Special Agent with the United States Secret Service (USSS), New York Field Office, Financial Crimes Task Force. I have been employed, in various capacities, by the USSS since 2009. In 2017, I transitioned to the position of Special Agent. As a USSS Special Agent, I am charged with investigating violations of the laws of the United States, collecting evidence in cases in which the United States is or may be a party of interest, and performing other duties imposed by law. More specifically, I conduct criminal investigations pertaining to financial obligations of the United States. As part of my responsibilities, I have attended various trainings including a 12-week Criminal Investigator Training Program at the Federal Law Enforcement Training Center and a 16-week Special Agent Training Course at the USSS's James J. Rowley Training Center.

2. The facts set forth in the affidavit are based upon my own personal observations, training and experience, as well as information obtained during this investigation from other sources, including (a) other agents from the USSS, and other law enforcement personnel involved in this investigations; (b) statements made or reported by various witnesses with personal

knowledge of relevant facts; and (c) my review of records obtained during the course of this investigation, as well as summaries and analyses of such documents and records that have been prepared by others.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Because this affidavit is submitted for the limited purpose of obtaining this search warrant, I have not set forth each and every fact I have learned in connection with this investigation. Where conversations and events are referred to herein, they are related in substance and in part, and where figures and calculations are set forth herein, they are approximate.

4. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below (the “SUBJECT PREMISES”) for, and to seize, the items and information described in Attachment B.

B. The SUBJECT PREMISES

5. The SUBJECT PREMISES is a light-brown colored, single-family, two-story, detached home, with a white door in the center with three steps leading up to it. When viewed from Oakmont Road, there are two windows to the right of the front door and a large bay window to the left of the front door. On the second level, there are three windows facing the street. There is a driveway to the right of the house that provides vehicle access to Laurel Street. The street address for the SUBJECT PREMISES is 4 Oakmont Road, Beverly, MA 01915. An additional description of the SUBJECT PREMISES is included in Attachment A.

6. Based on a review of subscriber records from Comcast, the registered subscriber at the SUBJECT PREMISES is CATHERINE PEARSON.

7. Based on a review of CATHERINE PEARSON's 2018 W-2 Wage and Tax Statement, CATHERINE PEARSON provided the address of the SUBJECT PREMISES as her home address.

8. Based on a review of public records, CATHERINE PEARSON is married to JAMES PEARSON.

9. Based on a review of JAMES PEARSON's 2018 W-2 Wage and Tax Statement, JAMES PEARSON provided the address of the SUBJECT PREMISES as his home address.

10. Based on a review of records for CATHERINE PEARSON's Fidelity Investments Retirement Savings, the SUBJECT PREMISES is CATHERINE PEARSON's home address.

11. Based on a review of records for JAMES PEARSON's Fidelity Investments Retirement Savings, the SUBJECT PREMISES is JAMES PEARSON's home address.

12. Based on DMV records, CATHERINE PEARSON's vehicle, a 2013 Gray Dodge Journey, with a Massachusetts license plate, number 327TN7, is registered to her at the SUBJECT PREMISES (the "VEHICLE").

13. Based on DMV records, JAMES PEARSON's vehicle, a 2012 Red Dodge Ram Truck, with a Massachusetts license plate, number 292XY6, is registered to him at the SUBJECT PREMISES.

14. On or about September 23, 2019, CATHERINE PEARSON was observed in the VEHICLE, parking in the driveway of the SUBJECT PREMISES, and entering and exiting the SUBJECT PREMISES.

15. Thus, there is probable cause to believe that both JAMES PEARSON and CATHERINE PERASON (together the "TARGETS") currently reside at the SUBJECT

PREMISES with their children, CLOEY PEARSON, LOGAN PEARSON and ETHAN PEARSON. An image depicting the SUBJECT PREMISES is included below:



C. The Subject Offenses

16. For the reasons detailed below, there is probable cause to believe the SUBJECT PREMISES contains evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 1341 (mail fraud), 1349 (conspiracy to commit wire fraud), 2320(a)(4) (conspiracy to commit trademark counterfeiting), and 1956 (laundering of monetary instruments).

D. Manufacturer Coupon Counterfeiting

17. Legitimate manufacturer coupons are issued by manufacturing companies, such as Procter and Gamble, to consumers with a save value embedded in the barcode. Manufacturer coupons contain certain terms and disclaimers indicating that they are not to be transferred, sold, reproduced or altered, and that doing so is illegal. There are many online communities dedicated to the creation, replication and/or alteration of coupons. There are various websites and blogs dedicated to instructing consumers how to effectively “glitch, glitter or balance” coupons, all terms

referring to the illegal, and intentional, misuse of coupons. Many of these websites lead to forums and social media groups dedicated to the buying and trading of counterfeit coupons.

E. Manufacturer Coupon Processing

18. When a customer makes a purchase and utilizes manufacturer coupons, the coupons provided are accepted by the retailer and the discount is applied by the retailer to the consumer at the time of payment. The retailer then sends the redeemed coupon to their clearinghouse, which is a processing center for all manufacturer coupons redeemed at the retailer. At the clearinghouse, the coupons are scanned to determine if they are legitimate or counterfeit. This is determined by an offer code, a unique six-digit identifier embedded in the barcode of every coupon. Offer codes are established by the manufacturer. If the offer code does not exist or is redeemed for a value other than the manufacturer's intended value, the coupon is flagged as counterfeit. The clearinghouse tallies all the redeemed coupons and generates an invoice which is sent to the manufacturer indicating how much is owed to the retailer for all redeemed coupons. From there, the manufacturer makes a reimbursement decision on which coupons they will reimburse the retailer for based on their legitimacy.

F. Background Regarding Social Media

19. PayPal is a technology platform company that enables peer to peer digital and mobile payments on behalf of consumers and merchants worldwide. PayPal allows its users to connect and transact online, on a mobile device, in an app, or in person.

20. Cash App, formerly known as Square Cash, is a mobile payment service developed by Square, Inc. CashApp allows its users to conduct electronic money transfers via debit card, credit card, or stored balance to other individuals and businesses within the United States.

21. Instagram is a social media networking platform and application which enables its users the ability to create, connect, communicate, and share information.

22. Venmo is a service of Paypal Inc., a licensed provider of money transfer services. Venmo requires its users to link a financial account to the application in order for the user to conduct peer to peer payments, provide payment to another mobile applications, or make direct deposits to a bank account.

23. Telegram is an encrypted cloud-based messaging application that allows its users to send multimedia files, establish device-specific 'secret chats' with self-destructing messages, photos, and videos, and create a platform to accept payments from users around the world.

G. Identification of the Targets

24. All subpoenaed financial records and law enforcement database inquiries indicate CATHERINE PEARSON, JAMES PEARSON, CLOEY PEARSON, LOGAN PEARSON and ETHAN PEARSON reside at the SUBJECT PREMISES.

25. A T-Mobile bill, from on or about May 26, 2019, and law enforcement database inquires positively associate the phone numbers ending in 4464 (herein the "4464 Number"), 2225 (herein the "2225 Number"), 7948 (herein the "7948 Number") and 7949 (herein the "7949 Number") to CATHERINE PEARSON and JAMES PEARSON at the SUBJECT PREMISES.

26. According to Comcast records from on or about February 14, 2019, subscriber information for the SUBJECT PREMISES indicates the subscriber name as CATHERINE PEARSON with the registered IP address of "73.143.79.13" (herein the "TARGET IP ADDRESS").

27. According to Google records, between July 2017 and December 2018, both dates being approximate and inclusive, the following e-mail addresses were registered and/or accessed by a user at the TARGET IP ADDRESS: "blinkieguy@gmail.com", "karenchen4445@gmail.com", "4bbq4445@gmail.com", "5journey4445@gmail.com",

“blinkman4445@gmail.com”, “jamespearson101@gmail.com”, “5dodge4445@gmail.com”, “dontblink4445@gmail.com”, and “newsblink4445@gmail.com”.

28. According to Google records from on or about January 21, 2019, “dontblink4445@gmail.com” and “4bbq4445@gmail.com” are linked to the 4464 Number, “jamespearson101@gmail.com” is linked to the 2225 Number, and “blinkman4445@gmail.com” is linked to the 7949 Number.

29. According to PayPal records, between April 2017 and January 2019, both dates being approximate and inclusive, the following e-mail addresses were registered and/or accessed by a user at the TARGET IP ADDRESS: “5journey445@gmail.com”, “5dodge4445@gmail.com”, “karenchen4445@gmail.com”, “newsblink4445@gmail.com”, “dontblink4445@gmail.com”, “jamespearson101@gmail.com”, and “blinkman4445@gmail.com”.

30. According to Venmo records from on or about April 23, 2019, subscriber information for “Jose-Chen” indicates the account is registered to “blinkieguy@gmail.com” and to the 2225 Number. Between March 2018 and August 2018, both dates being approximate and inclusive, the account was accessed by a user at the TARGET IP ADDRESS.

31. According to CashApp records from on or about May 31, 2019, subscriber information for the CashApp user “blinkieguy” indicates the account was registered to “Catherine Pearson”, “blinkieguy@gmail.com”, the 4464 Number and the SUBJECT PREMISES. Subscriber information for the CashApp user “kittykatmichelle” indicates the account was registered to “Catherine Pearson”, “4bbq4445@gmail.com”, and the SUBJECT PREMISES.

32. According to Instagram records, from on or about August 23, 2018, subscriber information for the Instagram user “blinkie_guy” indicates the account was registered to

“karenchen4445@gmail.com” and to the 7949 Number, and it was registered using the TARGET IP ADDRESS.

33. Between January 2018 and August 2018, both dates being approximate and inclusive, Instagram users “that_blinkieguy”, “blinkieguy”, “newnumberwhodis5”, “dontblink5555555” and “blinkie_guy”, requested and received payment for coupon orders via the PayPal accounts “blinkieguy@gmail.com” and “blinkman4445@gmail.com”, which are both associated by the TARGET IP ADDRESS with the SUBJECT PREMISES, or the CashApp account “blinkieguy”, which is registered to CATHERINE PEARSON and the SUBJECT PREMISES.

34. Between February 2018 and March 2018, both dates being approximate and inclusive, Telegram user “IP Machine” was the administrator for a group “Bible Study”. “IP Machine” posted requests for coupon order payment via the CashApp account “blinkieguy,” which is registered to CATHERINE PEARSON and the SUBJECT PREMISES.

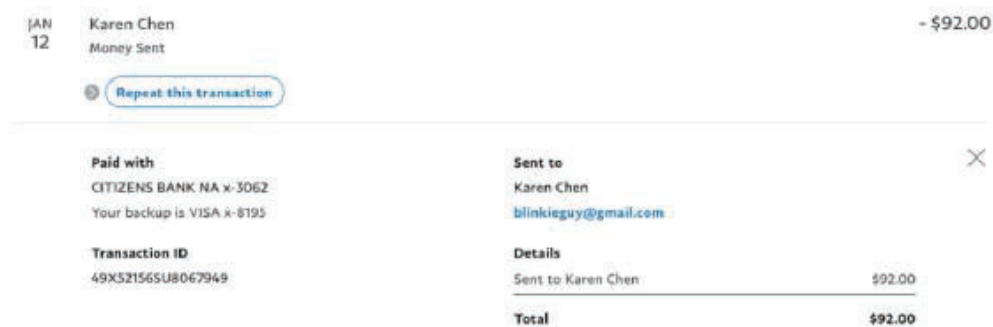
35. Between April 2018 and August 2018, both dates being approximate and inclusive, Telegram channel “SS, Blinkies, and Newsprint” posted requests for coupon order payment via the CashApp account “blinkieguy”, registered to CATHERINE PEARSON and the SUBJECT PREMISES, and the Venmo account “Jose-Chen”, which is also associated with the SUBJECT PREMISES.

H. Known Sales by Targets

36. There is probable cause to believe that, between January 2018 and August 2018, both dates being inclusive, an undercover buyer (herein the “UCB”) made eight (8) counterfeit manufacturer coupon purchases from the TARGETS, resulting in the acquisition of 449 counterfeit

manufacturer coupons.¹ The UCB spent \$581.00 for these coupons and received \$9,139.44 in manufacturer coupon value. In other words, for every \$1.00 spent for the purchase of counterfeit manufacturer coupons, the UCB received \$15.73 in manufacturer coupon value.

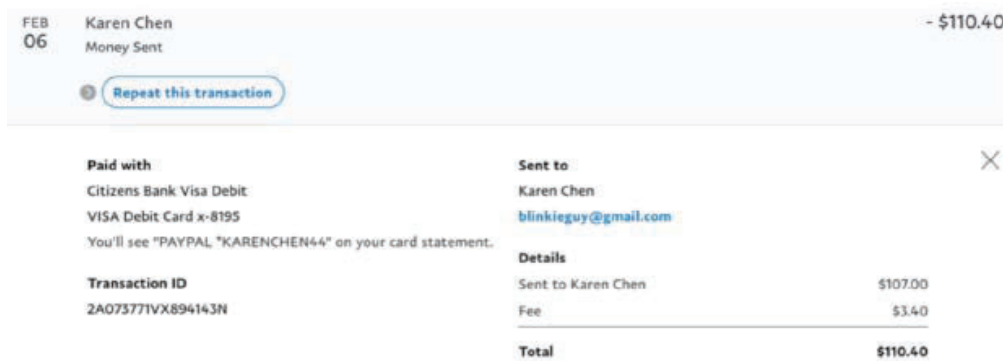
37. On January 12, 2018, the UCB placed an order for manufacturer coupons via a Google Form, titled “Blinkie Order Form”, posted in the profile of Instagram user “that_blinkieguy” (“Buy 1”). On January 12, 2018, the UCB sent payment, via PayPal, to “blinkieguy@gmail.com”, which is associated with the PayPal account ending in 2924 (herein the “2924 PayPal Account”). This account is registered to Catherine Strickland, which is the maiden name of CATHERINE PEARSON, and is associated with the TARGET IP ADDRESS. The 2924 PayPal Account utilized the TARGET IP ADDRESS to log in fifty-two (52) times between January 2018 and February 2018, both dates being approximate and inclusive. The package was shipped via the United States Postal Service (USPS) from Beverly, MA. A picture of the order and package is below.



¹ The UCB is employed by Brand Technologies, Inc. (“BT”), whose clients include, Proctor & Gamble and Clorox Services Company. BT is an international fraud and risk mitigation company that discovers, preserves and analyzes both digital and hard copy counterfeit coupons. BT is compensated by their clients to combat fraudulent coupons. To date, the information that has been provided to law enforcement, by BT, has proven reliable and been corroborated by independent investigation.

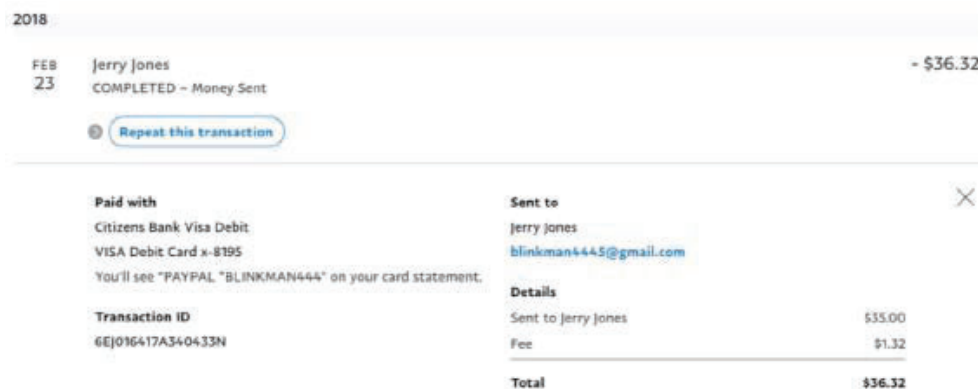


38. On February 5, 2018, the UCB placed an order for manufacturer coupons via a Google Form, titled “Blinkie Order Form”, posted in the profile of Instagram user “that_blinkieguy” (“Buy 2”). On February 6, 2018, the UCB sent payment, via PayPal, to “blinkieguy@gmail.com.” The package was shipped via USPS from Nashua, NH. A picture of the order and package is below.



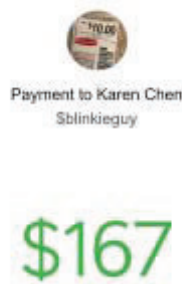


39. On February 23, 2018, the UCB placed an order for manufacturer coupons via a Google Form, titled “Blinkie Order Form”, posted in the profile of Instagram user “blinkieguy” (“Buy 3”). On February 23, 2018, the UCB sent payment, via PayPal, to “blinkman4445@gmail.com”, which is associated with a PayPal account ending in 2680, (herein the “2680 PayPal Account”). The 2680 PayPal Account utilized the TARGET IP ADDRESS to log in eighty-four (84) times between February 2018 and March 2018, both dates being approximate and inclusive. The package was shipped via USPS from Middle-Essex, MA. A picture of the order and package is below.

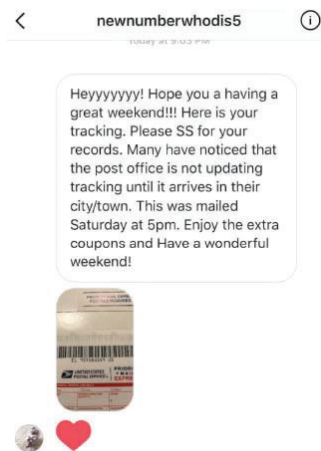
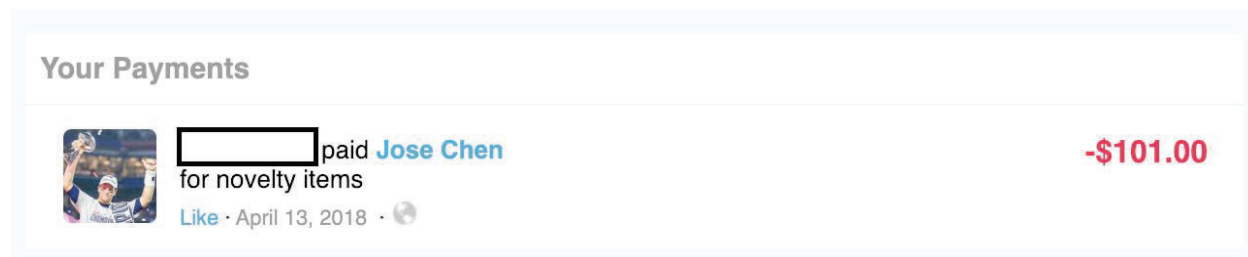




40. On March 27, 2018, the UCB placed an order for manufacturer coupons via a Google Form, titled “Blinkie Order Form”, posted in the profile of Instagram user “blinkieguy” (“Buy 4”). On March 27, 2018, the UCB sent payment, via CashApp, to the cashtag, “\$blinkieguy” per the order form instructions. The cashtag, “\$blinkieguy” is registered to CATHERINE PEARSON and to the SUBJECT PREMISES, with a registered alternate name of Karen Chen. The package was shipped via USPS from Beverly, MA. A picture of the payment message and package is below.



41. On April 13, 2018, the UCB placed an order for manufacturer coupons via a Google Form, titled “Blinkie Order Form”, posted in the profile of Instagram user “newnumberwhodis5” (“Buy 5”). On April 13, 2018, the UCB sent payment, via Venmo, to “blinkieguy@gmail.com”, which is associated with the TARGET IP ADDRESS, per the order form instructions. The package was shipped via USPS from Middle-Essex, MA. A picture of the Venmo communication, payment, and tracking information is below.



04/13/18

POS Debit

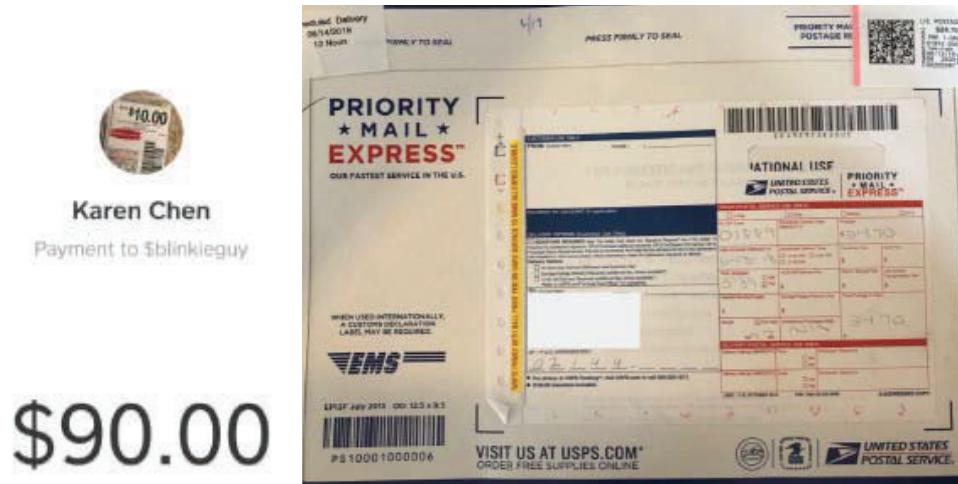
- \$101.00

Venmo* Visa Direct Ny 8195

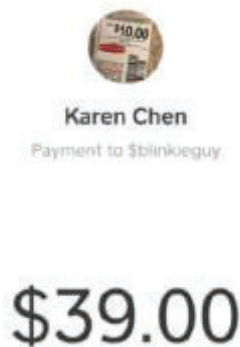
42. On May 8, 2018, the UCB placed an order for manufacturer coupons via a Google Form, titled “Blinkie Order Form”, posted in the profile of Instagram user “don’t_blink555555” (“Buy 6”). On May 8, 2018, the UCB sent payment, via CashApp, to the cashtag “\$blinkieguy”, per the order form instructions. The cashtag, “\$blinkieguy” is registered to CATHERINE PEARSON and to the SUBJECT PREMISES, with a registered alternate name of Karen Chen. The package was picked up by a USPS employee for shipment. According to USPS records from on or about May 17, 2018, the package was picked up at a latitude/longitude of (42.57878216, -70.88132083). The latitude/longitude is located at the SUBJECT PREMISES. Pictures of the CashApp message and tracking information are below.



43. On June 12, 2018, the UCB placed an order for manufacturer coupons via a Google Form, titled “Blinkie Order Form”, posted in the profile of Instagram user “blinkie_guy” (“Buy 7”). On June 12, 2018, the UCB sent payment, via CashApp, to cashtag “\$blinkieguy”, per the order form instructions. The cashtag, “\$blinkieguy” is registered to CATHERINE PEARSON and to the SUBJECT PREMISES, with a registered alternate name of Karen Chen. The package was shipped via USPS from Middle-Essex, MA. Pictures of the CashApp message and package are below.



44. On August 10, 2018, the UCB placed an order for manufacturer coupons via a Google Form, titled “Blinkie Order Form”, posted in the profile of Instagram user “blinkie_guy” (“Buy 8”). On May 10, 2018, the UCB sent payment, via CashApp, to cashtag “\$blinkieguy”, per the order form instructions. The cashtag, “\$blinkieguy” is registered to CATHERINE PEARSON and to the SUBJECT PREMISES with a registered alternate name of Karen Chen. The package was shipped via USPS from Nashua, NH. A photo of the payment communication is below.



45. The Google Form, titled “Blinkie Order Form” for Buy 1 1 offered manufacturer “Blinkie” style coupons only.

46. The Google Form, titled “Blinkie Order Form” for Buy 2, Buy 3, Buy 4, Buy 5, Buy 6, Buy 7 and Buy 8, offered numerous types of manufacturer coupons for purchase, to include: “Blinkies”, “Newsprints”, “Internet Printables”, “Catalinas” and Mobile “Screenshots”. In and of

itself, the sale and/or purchase of manufacturer coupons, constitutes coupon fraud. In addition, the order form allowed customers to request custom “Blinkies” and “Newsprints”. Custom “Blinkies” and “Newsprints” cannot be authentically created by any persons or entities other than the manufacturing company.

47. Between February 2018 and August 2018, both dates being approximate and inclusive, the Telegram user “IP Machine” and the channel administrator “SS, Blinkies & Newsprint” each publicized their ability to make coupons via social media. The below images are a sample of these references.



IP Machine
Yep! Just made it as a \$10 coupon



IP Machine
Read the order form please

Who else needs this? I'll make this with three month expiration



IP Machine
Anyone have a nestle water coupon?



Like this ?

Just need it emailed to blinkieguy@gmail.com
(mailto:blinkieguy@gmail.com)



SS, Blinkies & Newsprint
New template will be like this



SS, Blinkies & Newsprint



IP Machine
I offer an ip group that is \$30/ month fee
Everyone chooses 3 custom ips and gets access to everyone else's ips
20 members = 60 ips for \$30



IP Machine
Making Brawny \$3, \$7, \$10
Ok to order

48. Between February 2018 and August 2018, both dates being approximate and inclusive, approximately \$93,614.45 was transferred into the TARGETS' Bank of America account ending in 5713 (the "5713 Account") from PayPal, Venmo, and CashApp with no apparent legitimate business purpose.

49. According to Bank of America records, on June 11, 2019, \$95,000.00 was transferred from the 5713 Account to the Bank of America account ending in 6016 (the "6016 Account"). The 6016 Account is held in the names of both ETHAN PEARSON and CATHERINE PEARSON. On June 17, 2019, \$95,100.00 was transferred from the 6016 Account to the 5713 Account. Thus, there is probable cause to believe that the targets are engaged in money laundering with the proceeds of their crimes.

I. Known Purchases by Targets

50. According to PayPal records, between October 2016 and June 2017, both dates being approximate and inclusive, JAMES PEARSON's PayPal account, ending in 9600 (herein the "9600 PayPal Account"), regularly paid for counterfeit coupons. This is supported by the "Notes" section, of these transactions, that includes couponing terms, such as "coupon(s)", "IP", "peelies", and "q". In one transaction, the "Notes" section reads "couponmama wants 20 coupons". Thus, there is probable cause to believe that the TARGETS purchased counterfeit coupons.

51. According to PayPal records, on or about March 28, 2017, the 9600 PayPal Account was used to purchase one (1) "EPSON TM-C600 Wireless Inkjet POS Coupon Printer M228A Catalina Marketing CMC-6" and twelve (12) "EPSON Catalina Coupon Ink Cartridges 100764-SJIC11P(CMC)". Payments for both purchases were made via instant transfers from the 5713 Account. The shipping address provided for both purchases was CATHERINE PEARSON at the

SUBJECT PREMISES. Based on my training, experience and knowledge of this investigation, these items are used to manufacture counterfeit coupons.

52. According to PayPal records, on or about May 5, 2017, the 9600 PayPal Account was used to purchase one (1) “Hologram Holographic security self-adhesive tape “original” 50mm (w) x 1 metre”. Payment for this purchase was made via instant transfer from the 5713 Account. The shipping address provided for the purchase was CATHERINE PEARSON at the SUBJECT PREMISES. Based on my training, experience and knowledge of this investigation, this item is used to manufacture counterfeit coupons, specifically those that have a holographic sticker security feature.

53. According to PayPal Records, on or about November 25, 2017, the 9600 PayPal Account was used to purchased one (1) “EPSON Catalina TM-C600 CMC6 Wireless Inkjet POS Coupon Printer”. Payment for this purchase was made via instant transfer from the 5713 Account. The shipping address provided for the purchase was JAMES PEARSON at the SUBJECT PREMISES. Based on my training, experience and knowledge of this investigation, this item is used to manufacture counterfeit coupons.

54. According to Amazon records, on or about June 6, 2018, an Amazon user named Karen Smith (herein the “Smith Account”) purchased ten (10) “Sax Plain White Newsprint Newspaper - 8 1/2 x 11 inches - Pack of 500 – White”. Payment for this purchase was made via CATHERINE PEARSON’s Bank of America Debit Card ending in 0908 (the “0908 Card”). The purchase was made by a user at the TARGET IP ADDRESS. The billing information provided for the purchase was CATHERINE PEARSON at the SUBJECT PREMISES. Based on my training, experience and knowledge of this investigation, this item is used to manufacture counterfeit coupons, specifically Newsprint coupons.

55. According to Amazon records, on or about June 6, 2018, the user of the Smith Account purchased one (1) “Brother TN-331 Standard Yield Toner Cartridge Set”. Payment for this purchase was made via the 0908 Card. The purchase was made from a user at the TARGET IP ADDRESS. The billing information provided for the purchase was CATHERINE PEARSON at the SUBJECT PREMISES. Based on my training, experience and knowledge of this investigation, this item can be used to manufacture counterfeit coupons.

56. According to Amazon records, on or about June 21, 2018, the user of the Smith Account purchased four (4) “V4INK Compatible Brother TN336 TN315 TN310 TN331 Black Cyan Magenta Yellow High Yield Toner Cartridge Set for Brother HL-L8350CDW HL-L8350CDWT HL-4150”. Payment for these purchases was made using the 0908 Card. The purchase was made from a user at the TARGET IP ADDRESS. The billing information provided for the purchase was CATHERINE PEARSON at the SUBJECT PREMISES. Based on my training, experience and knowledge of this investigation, these items can be used to manufacture counterfeit coupons.

J. Use of Counterfeit Coupons by Targets

57. On June 7, 2019, the USSS Boston Field Office executed a trash pull at the SUBJECT PREMISES. The agents obtained a receipt for PetSmart that indicated four (4) manufacturer coupons, valued at \$17.00 each, were used in a transaction. All of these coupons were determined to be counterfeit.

58. Law enforcement obtained surveillance video of CATHERINE PEARSON using the four (4) manufacturer coupons at PetSmart. The Nestle Corporation has confirmed to law enforcement that the coupons were counterfeit. A photo of one of the coupons and the related receipt is below.



59. After further review of CATHERINE PEARSON's PetSmart transaction history, it was determined that CATHERINE PEARSON used counterfeit manufacturer coupons at PetSmart stores in September of 2018, October 2018 and April of 2019.

60. On or about October 31, 2018, CATHERINE PEARSON used four (4) \$15.00 counterfeit manufacturer coupons at PetSmart. Church and Dwight has confirmed to law enforcement that the coupons were counterfeit.

61. On or about September 13, 2018, CATHERINE PEARSON used four (4) \$15.00 and four (4) \$17.00 counterfeit manufacturer coupons at PetSmart. Church and Dwight has confirmed to law enforcement that the \$15.00 coupons were counterfeit. The Nestle Corporation has confirmed to law enforcement that the \$17.00 coupons were counterfeit.

62. On or about April 17, 2019, CATHERINE PEARSON used one (1) \$50.00 counterfeit manufacturer coupon at PetSmart. NCH Marketing, on behalf of Royal Canin, has confirmed to law enforcement that the coupon was counterfeit. A photo of the coupon is below.



63. On July 26, 2019, agents of the USSS Boston Field Office executed a second trash pull at the SUBJECT PREMISES. The agents obtained two (2) receipts for Walgreen's Pharmacy, which indicated twenty-three (23) manufacturer coupons, with a total value of \$121.00, were used in the transactions. To date, almost one-half of the manufacturer coupons have been confirmed to be counterfeit by Brand Technologies (BT).

64. On or about July 16, 2019, CATHERINE PEARSON used sixteen (16) manufacturing coupons at Walgreen's Pharmacy. At this time, seven (7) of the manufacturing coupons, valued at a total of \$45.00, have been confirmed to be counterfeit.

65. On or about July 23, 2019, CATHERINE PEARSON used seven (7) manufacturing coupons at Walgreen's Pharmacy. At this time, four (4) of the manufacturing coupons, valued at a total of \$20.00, have been confirmed to be counterfeit.

66. Law enforcement obtained surveillance video of CATHERINE PEARSON using manufacturer coupons in the July 16, 2019 and July 23, 2019 Walgreen's Pharmacy transactions. After further review of CATHERINE PEARSON's transaction history, it was determined, between August of 2018 and September of 2019, CATHERINE PEARSON used 180 counterfeit manufacturer coupons with a total value of \$1,307.80.

K. Summary

67. Based on information obtained from BT, as of October 1, 2019, a loss of \$1,017,798.83 is attributed to the TARGETS. The loss represents four (4) of fifty (50) manufacturing companies that have been affected. A loss has not yet been determined for the other forty-six (46) affected manufacturing companies. The loss is attributed to the TARGETS because the manufacturing companies were able to identify the quantity of “coupons denied” for each unique offer code which was extracted from manufacturer coupons purchased by the UCB and manufacturer coupons that were publicly available to members of the TARGETS’ social media groups. To calculate the total loss of the operation, the quantity of “coupons denied” for each unique offer code is multiplied by the scanned value of each offer code, plus an additional \$0.08 handling fee per coupon – charged by the clearinghouses.

L. Probable Cause Justifying Search of SUBJECT PREMISES and Seizure of Evidence Including Computer Equipment and Data

68. As described above, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on computer hard drives or other storage media. Thus, I am also seeking authorization to search any computers, tablets, and smartphones inside the SUBJECT PREMISES, for which there is reason to believe they belong to the TARGETS, pursuant to Rule 41(e)(2)(B).

69. I submit that if a computer or storage medium belonging to either of the TARGETS is found in the SUBJECT PREMISES, there is probable cause to believe the records and templates specified in this warrant will be stored on that computer or storage medium, for at least the following reasons: record-keeping that was once done manually on paper is now often conducted electronically on spreadsheets or bookkeeping programs. Those programs and related documents

are stored on desktop computers, tablets, smartphones, zip disks and other electronic memory storage media. Moreover, the TARGETS may have communicated with other individuals or potential co-conspirators by e-mail, text message, or private message on phone applications. Furthermore, agents will likely be able to retrieve metadata concerning the messages and documents on the computing devices, which will provide such information as the date the documents were created, last edited and the user name of the person who created them. This evidence can assist agents in determining the sequence of events under investigation.

70. Furthermore, such evidence likely continues to exist on such computers and electronic devices because:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can

take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. While it is technically possible to delete this information, computer users typically do not erase or delete it, because special software is typically required for that task.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

e. In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs or portable hard drives.

71. **Forensic evidence:** This application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the SUBJECT PREMISES, for which there is a reasonable basis to believe is used by either of the TARGETS, because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file or a template that has been deleted from an publishing software). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record

additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the government to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Lastly, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates

to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

72. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

73. **Necessity of seizing or copying entire computers or storage media.** In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

74. **Nature of examination.** Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

75. Because their children share SUBJECT PREMISES as a residence, it is possible that the premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that there is reason to believe that either of the TARGETS utilizes devices at the SUBJECT PREMISES that technically belong to someone else, the warrant applied for would permit the seizure and review of those items as well.

76. As with any search warrant, I expect that these warrants will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

Unlocking Devices with Biometric Features

77. I know from my training and experience and my review of publicly available materials that some models of cellphones made by Apple and other manufacturers offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

78. **Touch ID.** On the Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. This is a feature that recognizes up to five fingerprints designated by the authorized user of the iPhone. A Touch ID sensor, a round button on the iPhone or iPad, can recognize fingerprints. The fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numerical password, whichever the device is configured by the user to require. The Touch ID feature only permits up to five attempts with a fingerprint before the device will require the user to enter a passcode.

79. Furthermore, in devices running an operating system that predates iOS 9.3, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the device will require the passcode or password programmed by the user and will not allow access to the device based on a fingerprint alone. In devices running operating system version iOS 9.3 or later, the Touch ID feature will not substitute for the use of a passcode or password if more than 8 hours have passed since the device has been unlocked and the passcode has not been used to unlock the device in the last 6 days; in other words, if more than 8 hours have passed since the device was accessed and the passcode or password has not been used to unlock the device in the last 6 days, the device will require the passcode or password programmed by the user and will not allow access to the device based on a fingerprint alone.

Similarly, Touch ID will not allow access if the device has been turned off or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful. For these reasons, it is necessary that, promptly upon the retrieval of cellular telephone subject to seizure, agents use the fingerprints and thumbprints of the device's user (i.e., CATHERINE PEARSON and/or JAMES PEARSON) to attempt to gain access to the relevant device. The government may not be able to obtain the contents of relevant device if those fingerprints are not used to promptly access the relevant device by depressing them against the Touch ID sensor.

80. Although I do not know which of the ten finger or fingers are authorized to access on the relevant device and only five attempts are permitted, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for Touch ID.

81. **Facial Recognition.** Based on my training and experience, I know that certain cellular telephones are equipped with a facial-recognition feature, which, if enabled, allows a user the ability to unlock the device using his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the "Trusted Face" registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

82. In my training and experience, users of cellular telephones often enable features such as Touch ID or Trusted Face because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in

some instances, these features are considered to be a more secure way to protect the device's contents.

83. The passcode or password that would unlock the cellular telephone subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the relevant cellular telephone, making the use of biometric features a means to execute the search authorized by this warrant.

84. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if those features are enabled. This can occur when a device has been restarted, inactive, or has not be unlocked for a certain period of time. Some of those limitations with respect to Touch ID are described above. Certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through biometric features such as Touch ID of Trusted Face may exist for only a short time.

M. The Application for a Search Warrant

85. Based on the foregoing, I respectfully submit there is probable cause to believe that the TARGETS are engaged in the Subject Offenses, and that evidence, fruits and instrumentalities of this criminal activity is likely to be found in the SUBJECT PREMISES and on computers and electronic media found in the SUBJECT PREMISES.

REQUEST FOR SEALING

86. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



KATE E. HANECAK
Special Agent
United States Secret Service

Subscribed and sworn to before me on November 4, 2019.



HON. DONALD L. CABELL
United States Magistrate Judge
District of Massachusetts



ATTACHMENT A

The premises to be searched (the “SUBJECT PREMISES”) are described as follows, and include all locked and closed containers found therein:

A residence, owned by CATHERINE PEARSON and JAMES PEARSON, located at 4 Oakmont Road, Beverly, MA 01915. The SUBJECT PREMISES is accessible by entering through the front door. The SUBJECT PREMISES is a light-brown colored, single-family, two-story, detached home, with a white door in the center with three steps leading up to it. When viewed from Oakmont Road, there are two windows to the right of the front door and a large bay window to the left of the front door. On the second level, there are three windows facing the street. There is a driveway to the right of the house.



ATTACHMENT B

The items to be seized from the SUBJECT PREMISES include the following evidence, fruits and instrumentalities of violations of, inter alia, 18 U.S.C. §§ 1341 (mail fraud), 1349 (conspiracy to commit wire fraud), 2320(a)(4) (conspiracy to commit trademark counterfeiting), 1956 (laundering of monetary instruments).

1. Documents containing information concerning the Subject Offenses, including, among others, letters; notes; tax returns, forms, or schedules; bank statements; records of purchases, withdrawals, or deposits; or wire instructions.
2. Documents containing information concerning the existence, location(s), or access information for bank accounts used in connection with the Subject Offenses and/or containing proceeds of unlawful activity.
3. Documents containing information concerning the finances of CATHERINE PEARSON and JAMES PEARSON.
4. Documents reflecting personal identifying information for individuals other than CATHERINE PEARSON and/or JAMES PEARSON.
5. Documents related to the creation or use of email or other accounts in the names of individuals other than CATHERINE PEARSON and/or JAMES PEARSON.
6. Falsified documents intended to facilitate or further the Subject Offenses, including, among others, contracts, term sheets, licenses, identity documents, balance sheets, tax documents, or accounting records.
7. Proceeds of the Subject Offenses, including United States currency.
8. Electronic devices potentially containing evidence, fruits, and/or instrumentalities of the Subject Offenses. Law enforcement officers executing this Warrant are specifically authorized to seize any such electronic device provided they have reason to believe that it belongs to or is used by CATHERINE PEARSON and/or JAMES PEARSON.

Search and Seizure of Electronically Stored Information

The items to be seized from the SUBJECT PREMISES also include any computer devices and storage media for which there is reason to believe are owned or utilized by CATHERINE PEARSON and/or JAMES PEARSON, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones,

digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

During the execution of this search warrant, law enforcement are authorized to do the following for any device seized: (1) press the owner's fingers (including thumbs) against the fingerprint scanner of the device; (2) hold the owner in place while holding the device in front of his or her face to activate the facial recognition feature; and/or (3) hold the owner in place while holding the device in front of his or her face to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

Once unlocked, seized devices may then be searched for the items described in numbers 1 through 8 above.

UNITED STATES DISTRICT COURT

for the
District of Massachusetts

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)) Case No. 19-mj-1274-DLC
the Premises at 4 Oakmont Drive., Beverly, MA, and Any)
Closed Containers/Items Contained Therein, and)
Electronic Devices.)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____ Massachusetts
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before November 17, 2019 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Donald L. Cabell
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued:

11/4/20 3:00pm



Judge's signature

City and state:

Boston, Massachusetts



Hon. Donald L. Cabell, United States Magistrate Judge

Printed name and title

Return

Case No.:

19-mj-1274-DLC

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

The premises to be searched (the “SUBJECT PREMISES”) are described as follows, and include all locked and closed containers found therein:

A residence, owned by CATHERINE PEARSON and JAMES PEARSON, located at 4 Oakmont Road, Beverly, MA 01915. The SUBJECT PREMISES is accessible by entering through the front door. The SUBJECT PREMISES is a light-brown colored, single-family, two-story, detached home, with a white door in the center with three steps leading up to it. When viewed from Oakmont Road, there are two windows to the right of the front door and a large bay window to the left of the front door. On the second level, there are three windows facing the street. There is a driveway to the right of the house.



ATTACHMENT B

The items to be seized from the SUBJECT PREMISES include the following evidence, fruits and instrumentalities of violations of, inter alia, 18 U.S.C. §§ 1341 (mail fraud), 1349 (conspiracy to commit wire fraud), 2320(a)(4) (conspiracy to commit trademark counterfeiting), 1956 (laundering of monetary instruments).

1. Documents containing information concerning the Subject Offenses, including, among others, letters; notes; tax returns, forms, or schedules; bank statements; records of purchases, withdrawals, or deposits; or wire instructions.

2. Documents containing information concerning the existence, location(s), or access information for bank accounts used in connection with the Subject Offenses and/or containing proceeds of unlawful activity.

3. Documents containing information concerning the finances of CATHERINE PEARSON and JAMES PEARSON.

4. Documents reflecting personal identifying information for individuals other than CATHERINE PEARSON and/or JAMES PEARSON.

5. Documents related to the creation or use of email or other accounts in the names of individuals other than CATHERINE PEARSON and/or JAMES PEARSON.

6. Falsified documents intended to facilitate or further the Subject Offenses, including, among others, contracts, term sheets, licenses, identity documents, balance sheets, tax documents, or accounting records.

7. Proceeds of the Subject Offenses, including United States currency.

8. Electronic devices potentially containing evidence, fruits, and/or instrumentalities of the Subject Offenses. Law enforcement officers executing this Warrant are specifically authorized to seize any such electronic device provided they have reason to believe that it belongs to or is used by CATHERINE PEARSON and/or JAMES PEARSON.

Search and Seizure of Electronically Stored Information

The items to be seized from the SUBJECT PREMISES also include any computer devices and storage media for which there is reason to believe are owned or utilized by CATHERINE PEARSON and/or JAMES PEARSON, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones,

digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

During the execution of this search warrant, law enforcement are authorized to do the following for any device seized: (1) press the owner's fingers (including thumbs) against the fingerprint scanner of the device; (2) hold the owner in place while holding the device in front of his or her face to activate the facial recognition feature; and/or (3) hold the owner in place while holding the device in front of his or her face to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

Once unlocked, seized devices may then be searched for the items described in numbers 1 through 8 above.